# SYSTEMS AND METHODS FOR AUTHORIZING, AUTHENTICATING AND ACCOUNTING USERS HAVING TRANSPARENT COMPUTER ACCESS TO A NETWORK USING A GATEWAY DEVICE

## CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority from U.S. Provisional Patent Application Serial Number 60/111,497, the contents of which are incorporated by reference.

## FIELD OF THE INVENTION

The present invention relates generally to a gateway device and, more particularly, to a universal network gateway for enabling a computer to transparently access and communicate with a service provider network.

## BACKGROUND OF THE INVENTION

In order for a computer to function properly in a network environment, the computer must be appropriately configured. Among other things, this configuration process establishes the protocol and other parameters by which the computer transmits and receives data. In one common example, a plurality of computers are networked to create a local area network (LAN). In the LAN, each computer must be appropriately configured in order to exchange data over the network. Since most networks are customized to meet a unique set of requirements, computers that are part of different networks are generally configured in different manners in order to appropriately communicate with their respective networks.

While desktop computers generally remain a part of the same network for a substantial period of time, laptops, handhelds, personal digital assistants (PDAs), cellphones or other portable computers (collectively "portable computers") are specifically designed to be transportable. As such, portable computers are connected to different networks at different times depending upon the location of the computer. In a common example in which the portable computer serves as an employee's desktop computer, the portable computer is configured to communicate with their employer's network, i.e., the enterprise network. When the employee travels, however, the portable computer may be connected to different networks that communicate in different manners. In this regard, the employee may connect the portable computer to the network maintained by an airport, a hotel, a cellular telephone network operator or any other locale in order to access the enterprise network, the Internet or some other on-line service. The portable computer is also commonly brought to the employee's residence where it is used to access various networks, such as, the enterprise network, a home network, the Internet and the like. Since these other networks are configured somewhat differently, however, the portable computer must also be reconfigured in order to properly communicate with these other networks. Typically, this configuration is performed by the user each time that the portable computer is connected to a different network. As will be apparent, this repeated reconfiguration of the portable computer is not only quite time consuming, but is also prone to errors. The reconfiguration procedure may even be beyond the capabilities of many users or in violation of their employer's IT policy. Accordingly, special software must also typically be loaded onto the user's computer to support reconfiguration.



now abandoned. RW 3/29/04

As described by United States Patent Application No. 08/816,174 and United States Provisional Patent Application Nos. 60/111,497, 60/160,973, 60/161,189, 60/161,139, 60/160,890 and 60/161,182, a universal subscriber gateway device has been developed by Nomadix, Inc. of Westlake Village, California. The contents of these applications are incorporated herein by reference. The gateway device serves as an interface connecting the user to a number of networks or other online services. For example, the gateway device can serve as a gateway to the Internet, the enterprise network, or other networks and/or on-line services. In addition to serving as a gateway, the gateway device automatically adapts to a computer, in order that it may

communicate with the new network in a manner that is transparent both to the user and the new network. Once the gateway device has appropriately adapted to the user's computer, the computer can appropriately communicate via the new network, such as the network at a hotel, at home, at an airport, or any other location, in order to access other networks, such as the enterprise network, or other online services, such as the Internet.

The portable computer user, and more specifically the remote or laptop user, benefits from being able to access a myriad of computer networks without having to undergo the time-consuming and all-too-often daunting task of reconfiguring their host computer in accordance with network specific configurations. In addition, no additional software need be loaded onto the computer prior to connection to the other network. From another perspective, the network service provider benefits from avoiding "on-site" visits and/or technical support calls from the user who is unable to properly re-configure the portable computer. In this fashion, the gateway device is capable of providing more efficient network access and network maintenance to the user and the network operator.

Gateway devices are typically used to provide network access to the remote portable computer user, such as users in hotels, airports and other locations where the remote portable computer user may reside. Additionally, gateway devices have found wide-spread use in multi-resident dwellings as a means of providing the residents an intranet that networks the residents, broadband Internet access and the capability to adapt to the variances of the resident's individual enterprise networks. With the advent of even smaller portable computing devices, such as handhelds, PDAs, and the like, the locations where these users may reside becomes almost limitless.

User access to computer networks has been traditionally based upon the identity of the computer or computer user rather than the location of the accessing computer. For example, in conventional dial up modem access to computer networks, such as the Internet, a user must typically enter identification information such as the user's name and password. This user input information is then compared to a database of user profiles to determine if the user should be granted access. The database may also indicate the type of access and other related information, such as fees due. For example, where a subscriber to an Internet Service Provider (ISP) has purchased Internet access, a user profile database may contain information which not

only enables the user to be authenticated, but tracks the user's access for accounting purposes, such as maintaining a history of the user's access time on the network.

However, where the location-based access is established, access to the network cannot be based upon an individual user or computer, as multiple persons can obtain access from a given location, possibly utilizing different computers. Moreover, requiring each user to enter identification information for access overrides any convenience offered by simple, transparent location-based access to computer networks. Transparent network access is also impeded where access is not based upon location-based identification, but rather based upon user input identification information, where the gateway device enables a user to access networks based upon the user's computer settings. For instance, if a user's computer is configured to access a home network, identifying the computer may require the computer to be reconfigured.

Typical network access servers typically allow access to a server based upon a user's information, such as a user name. Authentication was typically done via a user name and password, which is an all or nothing approach. In other words, a user is either allowed access or denied access to a network. Therefore, user's can not be dynamically authorized access to a network such that the user's access and authorization to particular networks or sites can be determined and varied based upon attributes associated with the user, user's location, or packets received from the user's computer.

What is needed is an AAA method and system that allows users dynamic access based upon any number of variables, such as a user's location, a user name or password, a user's location. It would be advantageous for a user to be authorized access based on these variables. Furthermore, it would be advantageous for users to have flexible access to particular sites or services based upon these attributes. Therefore, an ISP or enterprise network can selectively permit access to users, and permit the user.

Therefore, an Authentication, Authorization and Accounting method and system would be desirable which enables a user transparent access to a computer network employing a gateway device, where the computer network can dynamically and selectively authorize a network access. Furthermore, authentication and access rights can be transparently based upon the location from which access is requested, or

based upon another attribute associated with the user's computer so that the user is not required to be queried for information and no additional configuration software need be loaded on the user's computer. Moreover, if the user is queried for access information, the user's data should be stored such that subsequent attempts to access the network do not require the user to establish authorization.

## SUMMARY OF THE INVENTION

The present invention comprises a method and system for selectively implementing and enforcing Authentication, Authorization and Accounting (AAA). The authentication capability can be based upon multiple methods. First, AAA can be done based upon where the traffic is originating, such as a location, computer, circuit, or user. Secondly, the authentication and authorization capability can be based upon the type of services the user is attempting to access, such as a destination address. This can be a destination port or Internet address, a TCP port, a network. Third, AAA can be based upon the content type or protocol being transmitted. For example, each packet can be filtered through the selective AAA process, so that a user can be authorized access to a particular location. Each time the user attempts to access a different location, the user is subject to the AAA, so the user may be prevented access from a particular site the AAA method deems inaccessible to the user based upon the user's authorization. Alternatively, the AAA method according to the present invention allows users to connect directly to a specific site, such as credit card or billing servers which collect billing information, which can indicate that the user has paid, so that the user is thereafter authorized access to networks. Additionally, a user's authorization can depend upon a specific time, so that the user can be kicked off a network at a specific time, after a specific time has elapsed, or according to other dynamic information determined by the network provider.

According to one embodiment of the invention, a method for transparently authorizing, authenticating and accounting users having access to a destination network is disclosed, wherein the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The method includes receiving at a gateway device a request from a user for access to the destination network and identifying an attribute associated with the user based

upon a packet received by the gateway device, wherein the packet is transmitted from the user's computer, wherein the user computer remains configured for accessing the home network, and wherein no additional configuration software need be installed on the user computer. The method also includes accessing a user profile corresponding to the user and stored in a user profile database, where the user profile is accessed based upon the attribute associated with the user, and determining if the user is entitled to access the destination network based upon the user profile.

According to one aspect of the invention, a location identifier is assigned to the location from which the request for access to the destination network is transmitted, where the location identifier is the attribute associated with the user. Thus, the packets received by the gateway device indicate the locations from which the requests were transmitted. The location identifier may be a virtual local area network (VLAN) ID assigned to the location from which the request for access was transmitted.

Furthermore, according to one aspect of the method of the present invention, the user profile database can be updated when new users access the destination network such that the user can be quickly authorized access once identified by a user name or password. Additionally, a historical log of user access to the destination network may be maintained in respective user profiles so that the system can accurately bill users for access to the destination network.

According to the method of the present invention, determining if the user is entitled to access the destination network can include denying the user access where the user's profile indicates that the user is denied access. However, the user may be directed to a login page in instances which the user's profile is not located within the user profile database.

According to another embodiment of the invention, a system for authorizing, authenticating and accounting users having transparent access to a destination network is disclosed, where the users otherwise have access to a home network through home network settings resident on the users' computers, and wherein the users can access the destination network without altering the home network settings. The system includes a gateway device for receiving a request from a user for access to the destination network, and means for identifying an attribute associated with the user based upon a packet received by the gateway device, wherein the packet is

transmitted from the user's computer, wherein the user's computer is configured for accessing the home network, and wherein no additional configuration software need be installed on the user computer. The system also includes a user profile database comprising stored access information that is in communication with the gateway device, wherein access information corresponding to the user is identified by the attribute associated with the user, and an Authentication, Authorization and Accounting (AAA) server in communication with the gateway device and user profile database, where the AAA server determines if user is entitled to access the destination network based upon the access information stored within the user profile database.

According to one aspect of the invention, the means for identifying can be provided by an access concentrator in communication with the gateway device. Furthermore, the packet transmitted to the gateway device can include a VLAN ID, a circuit ID, or a media access control (MAC) address for identifying the location from which the request for access was transmitted.

The user profile database includes a plurality of user profiles, wherein each respective user profile of the plurality of user profiles contains access information, and where each respective user profile contains historical data relating to the duration of destination network access for use in determining the charges due for the destination network access. Additionally, the user profile database can be located within the AAA server. The AAA server, can, in turn, be located within the gateway device.

The Authentication, Authorization and Accounting method and system according to the present invention enables users transparent access to a computer network employing a gateway device, where the computer network can authenticate and authorize access rights based upon the location from which access is requested, or based upon another attribute associated with the user in a manner transparent to the user. In this regard, the method and system of the present invention permit Authentication, Authorization and Accounting without requiring the user to reconfigure their computer and without requiring additional configuration software to be loaded upon the user's computer.

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a computer system that includes a gateway device for automatically configuring one or more computers to communicate via the gateway device with other networks or other online services, according to one embodiment of the present invention.

## DETAILED DESCRIPTION OF ONE EMBODIMENT OF THE INVENTION

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

Referring now to FIG. 1, a computer system **10** including a gateway device **12** is depicted in block diagram form. The computer system **10** typically includes a plurality of computers **14** that access a computer network in order to gain access to networks **20** or other online services **22**. For example, the computers **14** can be plugged into ports that are located in different rooms of a hotel, business, or a multi-dwelling unit. Alternatively, the computers **14** can be plugged into ports in an airport, an arena, or the like. The gateway device **12** provides an interface between the plurality of computers **14** and the various networks **20** or other online services **22**. One embodiment of a gateway device has been described by the aforementioned U.S. Patent Application No. 08/816,174.

Most commonly, the gateway device **12** is located near the computers **14** at a relatively low position in the overall network (i.e., the gateway device **12** will be located within the hotel, multi-unit residence, airport, etc.). However, the gateway device **12** can be located at a higher position in the system by being located closer to the various networks **20** or other online services **22**, if so desired. Although the gateway device **12** can be physically embodied in many different fashions, the gateway device **12** typically includes a controller and a memory device in which software is stored that defines the operational characteristics of the gateway device **12**. Alternatively, the gateway device **12** can be embedded within another network

device, such as an access concentrator **16** or a router **18**. For example, the gateway device **12** could be located at a network operating center or could be located before or after a router **18** in the computer network. Moreover, the software that defines the functioning of the gateway device **12** can be stored on a PCMCIA card that can be inserted into a computer of the plurality of computers **14** in order to automatically reconfigure the computer to communicate with a different computer system, such as the networks **20** and online services **22**.

The computer system **10** typically includes an access concentrator **16** positioned between the computers **14** and the gateway device **12** for multiplexing the signals received from the plurality of computers onto a link to the gateway device **12**. Depending upon the medium by which the computers **14** are connected to the access concentrator, the access concentrator **16** can be configured in different manners. For example, the access concentrator can be a digital subscriber line access multiplexer (DSLAM) for signals transmitted via regular telephone lines, a cable head end for signals transmitted via coaxial cables, a wireless access point (WAP) for signals transmitted via a wireless network, a cable modem termination shelf (CMTS), a switch or the like. As also shown in FIG. 1, the computer system **10** typically includes one or more routers **18** and/or servers (not shown in FIG. 1) to control or direct traffic to and from a plurality of computer networks **20** or other online services **22**. While the computer system **10** is depicted to have a single router, the computer system **10** can have a plurality of routers, switches, bridges, or the like that are arranged in some hierarchical fashion in order to appropriately route traffic to and from the various networks **20** or online services **22**. In this regard, the gateway device **12** typically establishes a link with one or more routers. The routers, in turn, establish links with the servers of other networks or other online service providers, such as internet service providers, based upon the user's selection. It will be appreciated by one of ordinary skill in the art that one or more devices illustrated in FIG. 1 may be combinable. For example, although not shown, the router **18** may be located entirely within the gateway device **12**.

Communication between users and networks or online services may be effectuated through ports, for example, located within hotel rooms or multi-dwelling units, or through conventional dial-up communications, such as through the use of telephone or cable modems. According to one aspect of the invention, users can be

are redirected to a portal page, as described below. After being redirected to the portal page, the user is subjected to a AAA process. Based upon the AAA process, the user may be permitted transparent access to the destination network or may be redirected to a login page in order to gather additional information to identify the user.

Identifying the user is crucial in authorizing access to networks or online services, as such services are typically provided for a fee and may be customized based upon the user, user's location, or user's computer. As such, the system of the present invention includes means for identifying a user based upon an attribute associated with the user that is contained within the packet transmitted from the user's computer. Attributes can include information such as the source, destination and type of traffic. In general, identifying a user's computer that accesses the network can be done by a MAC address associated with the user's computer. Identifying the a user accessing a network based upon a MAC address is well known to those of skill in the art, and will not be discussed in detail herein. Additionally, the attribute can be based upon a user name and ID, or according to one advantageous embodiment, a particular location, such as from a communications port in a hotel room. Such location-based identification in computer systems employing VLAN tagging and those not employing VLAN tagging according to the present invention will first be described. However, it should be appreciated that location based authorization is just one method of identifying a user which may be authenticated, authorized and accounted according to the present invention. As stated above, a user's computer can be identified based on a MAC address associated with the computer. A user can also be identified based upon a username and password. Additionally, a user can be identified according to a combination of these attributes.

The authentication capability can be based upon multiple methods. First, AAA can be done based upon where the traffic is originating, such as a location, computer, circuit, or user. Secondly, the authentication and authorization capability can be based upon the type of services the user is attempting to access, such as a destination address. This can be a destination port or Internet address, a TCP port, a network. Third, AAA can be based upon the content type or protocol being transmitted. For example, each packet can be filtered through the selective AAA process, so that a user can be authorized access to a particular location. Each time the user attempts to access a different location, the user is subject to the AAA, so the user

may be prevented access from a particular site the AAA method deems inaccessible to the user based upon the user's authorization. Alternatively, the AAA method according to the present invention allows users to connect directly to a specific site, such as credit card or billing servers which collect billing information, which can indicate that the user has paid, so that the user is thereafter authorized access to networks. Additionally, a user's authorization can depend upon a specific time, so that the user can be kicked off a network at a specific time, after a specific time has elapsed, or according to other dynamic information determined by the network provider.

Therefore, AAA can be based upon the source, destination, and type of traffic. Upon receiving a packet, the AAA module will look at various parameters such as the link layer information, such as the circuit, source MAC address, VLAN tag, circuit ID, along with network information such as source IP addresses, source port. This source information is stored into a AAA subscriber table. Secondly, information is gathered about the destination, such as the destination IP addresses, destination port, to determine what type of authentication is needed to access particular services. Third, the packet is interrogated to receive information such as the protocol type, port or the packet type to determine what type of authentication is required for a packet to be authorized for network access. Once this information is gathered, a matching of the authentication requirements versus the authorization is applied. If there is a match, the packet is forwarded and allowed access. If this match fails, the subscriber information for that packet is set as pending for authorization. Pending for authorization packets require further authentication and authorization before being allowed to access the system. Authorization can be determined based upon the attributes determined by the packet, or if not matched, the user will have to provide authentication, which can be done as described in the HPR patent, Serial Number _____, entitled "Systems and Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability " and incorporated herein by reference.

For example, once the gateway device identifies the location from which access is requested, such as from a specific port of a hotel room, the gateway device can then determine the access rights of the user at that specific location. It should be appreciated that as an alternative to location-based identification the gateway device

may identify a user or a user's computer based upon attributes other than location. For example, the gateway device may receive a MAC address identifying a particular user's computer (for example, a user in communication with the gateway device through a conventional modem), as is well known in the art, although the embodiments described herein will refer primarily to location-based identification as described above. Additionally, a user can be identified by the gateway device based upon a user ID and password which the user can input in response to a query for such information. This is discussed below and in U.S. Patent Application Serial Number _____, entitled "Systems and Methods For Redirecting Users Having Transparent Computer Access To A Network Using A Gateway Device Having Redirection Capability", filed concurrently with this application and incorporated herein by reference. In addition, a user staying in a particular hotel room may be authorized access based upon the user's location. Alternatively, the user can be authorized access to the network and online services based upon the user's identification, or the user's computer, regardless where the user is obtaining access. Furthermore, access may be associated with a combination of attributes. For example, a user may be authorized access to a network where the user has input the user's identification and has accessed the network from a particular room. Such a requirement could prevent unauthorized users also staying in a particular room from obtaining network access.

Regardless of the means in which access is obtained and an attribute associated with the user is identified, access rights of users are determined according to an AAA method implemented by a AAA server. According to one embodiment of the present invention, the AAA server is located entirely within the gateway device. Alternatively, the AAA server can also be located external to the gateway device.

One function of the AAA server is to identify the user in communication with the gateway device in a manner that is transparent to the user. That is, the user will not be required to reconfigure the computer or otherwise change the home network settings, and no additional configuration software will have to be added to the computer. After a packet is received by the gateway device, as described in detail above, information contained within the packet is stored within a subscription table. The subscription table is a database of user information. In particular, the subscription table can maintain any information or attribute known about a user,

including a circuit or MAC address, such that a particular user or user location can be identified upon accessing the computer system. After a packet is received, and attributes associated with a user are obtained, information corresponding to the packet is received from the subscription table. It will be appreciated by those of skill in the art that the packet may identify the location of the port from which access is obtained based upon location-based authorization, as described above, or a specific computer based upon a MAC address, as is well known in the art. Regardless of connection means however, any attribute or anything known about the user or location of the traffic, can be stored in the subscriber table. The subscription table and information stored therein may be stored in a computer readable storage medium, as well known in the art, that is either disposed within the gateway device or external.

After receiving a request for access from a user and identifying the user or location through the use of the subscription table, the AAA server then determines the access rights of the particular user. What is done with the user depends upon information contained in the user's profile. Profiles of all users (i.e., identified by MAC address or by location or by some other attribute) are stored in a user profile database, which may be located internal to or external to the gateway device. It will be appreciated by those of skill in the art that although the user profile database is discussed herein as being separate and distinct from the subscription table, the two databases may be combined into one database containing both user subscription data as well as user profile data.

The user's profile can contain information that is based upon the user or the user's location (as established by location-based identification), and generally includes information concerning the access rights of a user or location. For example, the user profile database may establish that a user with a given MAC address has purchased access, or that a given circuit ID has free access or unlimited access. Guests in a particular room or rooms of a hotel, for example, suites and penthouses, may receive free unlimited internet access. Therefore, access rights can be available contingent upon the user's location (e.g. room) or location status (e.g. suite). In this event, no further identification is required, as the location from which the users are requesting access is known to the gateway device and stored in the subscription table.

In addition to storing whether users have valid access rights, the user profile database can also include specialized access information particular to a specific

location or user, such as the bandwidth of the user's access, or a homepage to which a user should be directed. For example, a user accessing the network from a penthouse may receive a higher access band rate than someone accessing the destination network from a typical hotel room. Additionally, a user profile can include historical data relating to a user's access to the network, including the amount of time a user has accessed the network. Such historical information can be used to determine any fees which may be charged to the user, or due from the user, for access. Specialized access information contained within the user profile may be established by the system administrator, or by the user who has purchased or otherwise established access to the network. For example, where a user is transparently accessing the gateway device from a hotel room, the hotel network administrator may enter user access information into the profile database based upon access rights associated with a room in the hotel. This can also be done automatically by the gateway device or a local management system, such as a hotel property management system, when the user checks into his or her room. Additionally, the user may establish the information to be contained within the profile database upon first accessing the gateway device, as will be described in detail below. For instance, a new user may be directed to enter their credit card number to obtain access to the system. Whereas the subscription table initially identifies the user and maintains location information, the user profile database includes information concerning the details of the user's access privileges, as well as any specialized information for each user.

As noted above, user profile database can be maintained within the gateway device, or it can be located external to the gateway device. For example, where a hotel wishes to establish transparent network access for customers from hotel rooms, the hotel may maintain the profile database locally within the gateway device. Alternatively, if external to the gateway device, the profile database will can contain the same information and be accessed by the gateway device to ascertain user's access rights. According to one embodiment of the invention, the profile database can be maintained outside of the gateway device by an internet service provider.

Upon receiving the location of a port or identity of a user transparently communicating with the gateway device, the AAA server compares the identification information contained within the packet to user profile information stored within the user profile database. This comparison may be accomplished using a computer

having an operating system and software therein for comparing identification information in the received packet to records stored within the user profile database. Where users are not identified automatically based upon their location, the users may be required to identify themselves using a login and ID, so that their identification can be compared to user profiles stored within the user profile database. In an alternative embodiment of the present invention, the AAA server could query the user's computer, and more specifically, the user's browser, to obtain identification information stored therein so that the AAA server does not have to query a user for user information, thereby further making the AAA process of the present invention transparent to the user.

The user profile database may comprise programmable storage means located on a conventional personal computer, mainframe computer, or another suitable storage device known in the art. Additionally, the means for comparing the received data to the data within the database can comprise any software, such as an executable software program, which can compare data. For example, the AAA server may store user profiles on a hard drive of a personal computer, and the means for comparing the received user data to the user profiles resident on the computer can include computer software, such as Microsoft Excel (Microsoft Excel is a trademark of Microsoft Corporation, Redmond, Washington). According to another embodiment of the invention, the AAA server can comprise a remote authentication dial-in user service (RADIUS), which is a well known authentication and accounting system used by a number of network service providers (NSPs).

Once a user's profile has been determined by access to the user's profile in the user database, three possible actions can result. Specifically, once a user's profile has been retrieved the AAA server may determine a user to have access, to be pending or in progress, or to not have access.

First, a user is deemed valid (i.e., to have access) where the user's profile in the user profile database states so. If a user is determined to be valid, the user's traffic can be allowed to proceed out of the gateway device from the portal page to the networks or online services the user wishes to access, or the user may be redirected to a portal page, typically, a more user-specific portal page, as described in U.S. Patent Application Serial No. _____, entitled "Systems and Methods For Redirecting Users Having Transparent Computer Access To A Network Using A

Gateway Device [redacted]ing Redirection Capability, (hereinafter "[redacted]Redirecting Application") filed concurrently herewith, prior to being allowed access to the destination network. For example, a user may be automatically forwarded to a user-input destination address, such as an Internet address, for example, where a user has free access associated with the user's hotel room. Alternatively, this may occur where the user has already purchased access and the user has not exhausted available access time.

If the second scenario occurs, in which the user is deemed pending or 'in progress', the user may take steps to become authenticated so that the user's information may be recorded in the user profile database and the user is deemed valid. For example, a user may have to enter into a purchase agreement, requiring the user to enter a credit card number. If the user needs to purchase access, or if the system needs additional information about the user, the user can be redirected from the portal page via Home Page Redirect (HPR) and Stack Address Translation (SAT) to a location, such as a login page, established to validate new users. SAT and HPR can intervene to direct the user to a webserver (external or internal) where the user has to login and identify themselves. This process is described in detail below and in more detail in the Redirecting Application.

According to one illustrative example, a user profile database is maintained by an ISP which may be associated with the computer network for providing internet service to those users on the network. Although unlimited access could be granted to users based on their location or MAC address, access may also be limited based on the access for which a user has paid. For example, the user profile database may route a user to a login page, where the user must enter user data, such as a user id and password. In this embodiment, a network access server (NAS) **28**, located within the gateway device **12**, can receive user data. Upon receiving user data representing the identity of a user attempting to access the network, a primary function of the NAS **28** is to grant or deny the user access to the network.

Although the NAS **28** grants and denies access to users, the NAS **28** does not determine whether each user is allowed to connect to the network and, if so, what type of connection should be established. Rather, these determinations are made by the AAA server **30**, illustrated as exterior to the gateway device in FIG. 6, and described in detail above. Upon receiving user data the NAS **28** can, if necessary, reconfigure

the data such that the data will be in the proper format to be received by the AAA server **30**. In addition to reconfiguring the user data, the NAS **28** can also encrypt the user data such that the user identity and password will be protected during transmission to the AAA server **30**. After reconfiguration, and optionally, encryption, the NAS **28** transmits the data to the AAA server **30** with a query to request that the AAA server **30** authenticate the user.

The AAA server **30** stores user profiles corresponding to users authorized to access the network. The user profiles typically include user identifications, passwords, access authorization, billing, and other pertinent user information. The AAA server **30** compares stored user profiles with the user data received from the gateway device **12** to determine if the user should be granted access to the network. As such, the AAA server **30** generally comprises a database and data storage means. According to one embodiment of the invention, the AAA server **30** is maintained by an ISP. In this embodiment, the user profiles stored by the AAA server **30** establish those users that can obtain Internet access via the ISP network. The ISP edits user profiles within the AAA server **30** to reflect those users who may become authorized or unauthorized to access the network.

Continuing with the illustrative example, the ISP may only register user profiles in the authentication database after users have been identified by the ISP and necessary billing information, such as addresses and credit card numbers, have been submitted. If the ISP has not posted a user profile in the AAA server **30** at the time of authentication, the user will not be permitted access to the network. If this occurs, the user may be asked to submit profile information to the ISP so that the ISP can add the user's profile to the AAA server **30**. Furthermore, this may also be done the first time a user attempts to access the gateway device **12**. The information may be entered by the user with the aid of webpage, a pop-up control panel or user interface, which can open when the user initially connects to the gateway device **12**, as effectuated by HPR and SAT. As will be discussed below, the gateway device can request user information and forward it to the ISP such that the user does not know an ISP is receiving the information.

In the embodiment shown in FIG. 6, the AAA server **30** is located outside of the gateway device, although it may alternatively be located within the gateway device. For example, the location of the AAA server **30** may be such that the NAS **28**

communicates with the AAA server **30** via internet protocol. Therefore, it will be appreciated that the AAA server **30** may be located at any internet address and stored on any computer accessible via internet protocol. Locating the AAA server **30** outside of the network can provide a number of advantages. First, the administrative burden on the network is alleviated because the network does not have to set up and maintain separate authentication databases on each network or gateway device. This is especially important because each gateway device **12** allows a finite number of users to access the network, so that multiple gateway devices may be required. Secondly, administering and maintaining one consolidated database of authentication data is easier than multiple smaller databases.

Referring again to the illustrative AAA example, after any requisite reconfiguration, the NAS **28** can transmit user data to the AAA server **30** with a query to request that the AAA server **30** authenticate the user. The AAA server **30** receives the user data and then compares the received user data to user profiles stored within its database. Where a customer is not identified by location, establishing access to the gateway device will typically involve a process in which a user must enter their identity and a password, and in some instances a desired billing scheme and service level as offered by the gateway administrator or network operator (information hereinafter collectively referred to as user data). Additionally, the user data can include information such as a user's social security number and a credit card number. As described briefly above and in more detail below, the gateway device can direct the user to a webpage that requests desired data. However, where the customer is identified by location, the customer may only have to choose connection options, such as fixed fee or pay-per-use access, or a particular baud rate where the user can pay a premium for a higher speed connection, as the identity of the user may be known based upon location, and the user's payment information may already be known, such as where access is obtained via a port in a hotel room.

Assuming that a user has been deemed pending or 'in progress', the gateway device typically presents users with a login page that enables new users to subscribe to the computer network so that they may subsequently obtain transparent access to networks or online services transparently through the gateway device. To direct the users to a login page the AAA server calls upon a HPR function. The HPR directs the user to the login page, and after the user has entered requisite information into the

login page, the AAA server adds the new information to the customer profile database and can direct the user to the user's desired destination, such as an Internet address, or a portal page created by the network provider or users. Thus, new users can gain access to networks or online services without being predefined in the user profile database.

Because the gateway device is transparent to the user, the user communicates with the gateway device without the user's knowledge. This transparent communication results in a plug and play capability which enables a user to plug a computer into a port and directly access the internet or another online service without reconfiguring his or her computer from the home network settings resident on the computer and without requiring additional software to be loaded on the user computer. Therefore, the functions of the AAA server, and of HPR can be completely transparent to the user. For example, utilizing the system and method of the present invention, a user who has not purchased network access, and does not receive free network access, can plug into a port of the computer network and request connection to an Internet address through the user's Internet browser. After being directed to a portal page, the AAA server, unbeknownst to the user, identifies this user as pending (i.e., no information for that user has been identified in the user profile database), and calls upon the HPR function to send the user from the portal page to a login page which is different from the destination address initially entered by the user. Specifically, the HPR function as well as the SAT, discussed below, are performed by the AAA server and/or gateway device.

To achieve this redirection, HPR utilizes a SAT operation to direct the user from a portal page to a new destination at which a login page is presented, which is preferably local to the gateway device so that the redirection will be efficient and fast. This is accomplished by redirecting the user to a protocol stack using network and port address translation to the portal server that can be internal to the computer network or gateway device. More specifically, the AAA server receives the user's Hyper Text Transfer Protocol (HTTP) request for a web page and sends back the HTTP response reversing the network and port address translation the portal server, essentially acting as a transparent 'go-between' to the user and new webserver. It will be appreciated, however, that to receive the HTTP request the AAA server must

initially open a Transmission Control Protocol (TCP) connection to the another server in line with the user-requested internet address.

After receiving the user's login information, the AAA server will create a user profile utilizing this information so that the user will be able to obtain immediate access to the network next time the user logs in without being required to enter login information again. The AAA server can create a profile for the user in a locally stored user profile database, as described above, or can update the user profile in a database external to the gateway device. Regardless of the location of the user profile, the next time the user attempts to login the user's profile will be located in the user profile database, the user's access rights determined, and the user allowed transparent access to networks or services.

Many modifications and other embodiments of the invention will come to mind to one skilled in the art to which this invention pertains having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.